Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - AVIRA Antivirus Arbitrary Code Execution
  - CSystems WebArchiveX Arbitrary File Access
  - Eset NOD32 Arbitrary Code Execution
  - Ipswitch WhatsUp Multiple Vulnerabilities
  - Mall23 SQL Injection
  - Microsoft Exchange Server 2003 Denial of Service
  - **Microsoft Outlook Express Could Allow Remote Code Execution (Updated)**
  - SecureOL VE2 Security Restriction Bypass
  - KillProcess Arbitrary Code Execution
  - Sophos Anti-Virus Denial of Service
  - Yaosoft COOL! Remote Control Denial of Service
- UNIX / Linux Operating Systems
  - **Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass (Updated)**
  - Apple Mac OS X Java Update
  - **Astaro Security Linux HTTP CONNECT Unauthorized Access (Updated)**
  - **BlueZ Arbitrary Command Execution (Updated)**
  - Common-lisp-controller Elevated Privileges
  - **CVS 'Cvsbug.In' Script Insecure Temporary File Creation (Updated)**
  - **Eric Raymond Fetchmail POP3 Client Buffer Overflow (Updated)**
  - **GNU CPIO Archiver Insecure File Creation (Updated)**
  - **GNU CPIO CHMod File Permission Modification (Updated)**
  - **GNU CPIO Directory Traversal (Updated)**
  - GNU Mailutils Format String
  - **IBM AIX Multiple Buffer Overflows (Updated)**
  - **IBM AIX NIS Client Remote Arbitrary Code Execution (Updated)**
  - **Info-ZIP UnZip File Permission Modification (Updated)**
  - **KDE kcheckpass Superuser Privilege Escalation (Updated)**
  - **KDE langen2kvtml Insecure Temporary File Creation (Updated)**
  - Mark D. Roth PAM_Per_User Authentication Bypass
  - **Kismet Multiple Remote Vulnerabilities (Updated)**
  - **Multiple Vendors TLS Plaintext Password (Updated)**
  - **Multiple Vendors Zlib Compression Library Buffer Overflow (Updated)**
  - **Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service (Updated)**
  - **Multiple Vendors dhcpcd Denial of Service (Updated)**
  - **Multiple Vendors LibXPM Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors KAME Racoon Malformed ISAKMP Packet Headers Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Subthread Exec Denial of Service (Updated)**
  - Multiple Vendors Linux Kernel EXT2/EXT3 File Access Bypass
  - Multiple Vendors Linux Kernel 'Ipt_recent' Remote Denial of Service
  - Multiple Vendors Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service
  - Multiple Vendors FreeRADIUS Multiple Remote Vulnerabilities
  - Multiple Vendors KAudioCreator CDDB Arbitrary File Overwrite
  - **Multiple Vendors Gaim AIM/ICQ Protocols Buffer Overflow & Denial of Service (Updated)**
  - **Multiple Vendors XPDF Loca Table Verification Remote Denial of Service (Updated)**
  - **Multiple Vendors GNOME Evolution Multiple Format String (Updated)**
  - Multiple Vendors Linux Kernel SCSI ProcFS Denial of Service
  - Multiple Vendors Util-Linux UMount Remounting Filesystem Elevated Privileges
  - Multiple Vendors XFree86 Pixmap Allocation Buffer Overflow
  - **netpbm Arbitrary Code Execution (Updated)**
  - Open WebMail Cross-Site Scripting
  - **PCRE Regular Expression Heap Overflow (Updated)**
  - Snort 'PrintTcpOptions' Remote Denial of Service
  - Squid Aborted Requests Remote Denial of Service
  - **Squid 'sslConnectTimeout()' Remote Denial of Service (Updated)**
  - TMSNC Format String
  - **Vim Arbitrary Code Execution (Updated)**
- Multiple Operating Systems
  - **Apache HTTP Request Smuggling Vulnerability (Updated)**

- ATutor 'Password_Reminder.PHP' SQL Injection & Information Disclosure
- Azerbaijan Development Group AZDGDatingLite Directory Traversal
- CGI Central AMember Remote File Include
- Check Point SecurePlatform NGX Firewall Rules Bypass
- Cisco CSS 11500 Series SSL Authentication Bypass
- Class-1 Forum SQL Injection
- Crashcool.com PhpTagCool SQL Injection
- Distributed Checksum ClearingHouse DCCIFD Denial of Service
- **Ethereal Denial of Service or Arbitrary Code Execution (Updated)**
- Flowerfire Sawmill Cross-Site Scripting
- **HP OpenView Network Node Manager Remote Arbitrary Code Execution (Updated)**
- IBM OS/400 Multiple OSP-CERT Vulnerabilities
- IBM OS/400 Malformed SNMP Requests Remote Denial of Service
- Ingate Administrative Interface Cross-Site Scripting
- **KDE Kate, KWrite Local Backup File Information Disclosure (Updated)**
- Linksys WRT54G Wireless Router Multiple Remote Vulnerabilities
- Mimicboard2 Multiple HTML Injection & Unauthorized Access
- MIVA Merchant 5 Cross-Site Scripting
- **Mozilla Firefox Multiple Vulnerabilities (Updated)**
- Mozilla/Netscape/Firefox Browsers Domain Name Buffer Overflow
- **Multiple Vendors Apache Remote Denial of Service (Updated)**
- **Multiple Vendors PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution (Updated)**
- MyBulletinBoard SQL Injection Vulnerabilities
- **MySQL User-Defined Function Buffer Overflow (Updated)**
- **OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials (Updated)**
- **OpenVPN Multiple Remote Denials of Service (Updated)**
- PHPCommunityCalendar Multiple Remote Vulnerabilities
- **phpLDAPadmin Multiple Vulnerabilities (Updated)**
- PHPNuke Multiple SQL Injection
- PunBB Multiple Vulnerabilities
- Rdiff-backup Directory Access Insufficient Restrictions
- Mail-it Now! Upload2Server Arbitrary File Upload
- SMC SMC7904WBRA Wireless Router Remote Denial of Service
- Spymac Web OS Cross-Site Scripting
- Stylemotion WEB//NEWS Multiple SQL Injection
- Subscribe Me Pro S.PL Remote Directory Traversal
- Sun Java System Application Server JAR File Information Disclosure
- Sun Java Web Proxy Server Remote Denials of Service
- Symantec Brightmail Remote Denials of Service
- **TDiary Cross-Site Request Forgery (Updated)**
- **Unclassified NewsBoard Description Field HTML Injection (Updated)**
- Zebedee Remote Denial of Service

Wireless

Recent Exploit Scripts/Techniques

Trends

Viruses/Trojans

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
AVIRA Desktop for Windows 1.00.00.68 with AVPACK32.DLL version 6.31.0.3	A buffer overflow vulnerability has been reported in AVIRA Desktop for Windows, ACE archive processing, that could let remote malicious users execute arbitrary code. Update to AVPACK32.DLL version 6.31.1.7 using AVIRA's online update feature. Currently we are not aware of any exploits for this vulnerability.	AVIRA Antivirus Arbitrary Code Execution	High	Secunia, Advisory: SA16691, September 14, 2004
CSystems WebArchiveX 5.5.0.76	A vulnerability has been reported in WebArchiveX that could let remote malicious users access arbitrary files. Upgrade to a release after September 6th, 2005. There is no exploit code required.	CSystems WebArchiveX Arbitrary File Access CAN-2005-2891	Medium	Security Tracker, Alert ID: 1014867, September 7, 2005
Eset NOD32 Antivirus for Windows NT, 2000, 2003, XP, trial version 2.5 with nod32.002 version 1.033 build 1127	A buffer overflow vulnerability has been reported in NOD32, ARJ archive processing, that could let remote malicious users execute arbitrary code. Update to nod32.002 version 1.034 build 1132 using NOD32's online update feature. Currently we are not aware of any exploits for this vulnerability.	Eset NOD32 Arbitrary Code Execution CAN-2005-2903	High	Secunia, Advisory: SA16604, September 8, 2005
Ipswitch WhatsUp Gold 8.0 4, Whatsup Small Business 2004	Multiple vulnerabilities have been reported in WhatsUp that could let remote malicious users to disclose files, conduct Cross-Site Scripting, or arbitrary code execution. No workaround or patch available at time of publishing. There is no exploit code required.	Ipswitch WhatsUp Multiple Vulnerabilities	High	Security Focus, Bugtraq ID: 14792, 14797, 14799, September 9, 2005
Mall23 Mall23 eCommerce	An input validation vulnerability has been reported Mall23 eCommerce ('infopage.asp') that could let remote malicious users perform SQL injection. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Mall23 SQL Injection	Medium	Security Tracker, Alert ID: 1014882, September 12, 2005
Microsoft Exchange Server 2003	A vulnerability has been reported in Exchange Server 2003, Microsoft Exchange Information Store service, that could let remote malicious users cause a Denial of Service. Vendor hotfix available: http://support.microsoft.com/default.aspx/kb/840123 There is no exploit code required.	Microsoft Exchange Server 2003 Denial of Service	Low	Secunia, Advisory: SA16740, September 8, 2005
Microsoft Outlook Express 5.5, 6	A remote code execution vulnerability has been reported in Outlook Express when it is used as a newsgroup reader. A malicious user could exploit the vulnerability by constructing a malicious newsgroup server that could that potentially allow remote code execution if a user queried the server for news. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-030.mspx **An exploit script has been published.**	Microsoft Outlook Express Could Allow Remote Code Execution CAN-2005-1213	High	Microsoft, MS05-030, June 14, 2004 US-CERT VU#130614 **Security Focus, Bugtraq ID: 13951, September 12, 2005**
SecureOL VE2 1.05.1008	A vulnerability has been reported in VE2 that could let local malicious users bypass security restrictions. Upgrade to version 1.05.1009: http://www.download.com/VE2/3000-2653_4-10426897.html A Proof of Concept exploit script has been published.	SecureOL VE2 Security Restriction Bypass CAN-2005-2890	Medium	Secunia Advisory: SA16739, September 8, 2005
SoftTree Tech KillProcess prior to 2.20	A buffer overflow vulnerability has been reported in KillProcess that could let local malicious users to execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	KillProcess Arbitrary Code Execution	High	Security Focus, Bugtraq ID: 14795, September 9, 2005
Sophos Sophos AntiVirus	A vulnerability has been reported in Sophos Anti-Virus 'Scan Mailboxes' feature that could let remote malicious users cause a Denial of Service. Vendor workaround available: http://www.sophos.com/	Sophos Anti-Virus Denial of Service	Low	Security Tracker, Alert ID: 1014869, September 8, 2005

	support/knowledgebase/article/1691.html There is no exploit code required.			
Yaosoft COOL! Remote Control 1.12	A vulnerability has been reported in COOL! Remote Control that could let a local malicious users cause a Denial of Service. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Yaosoft COOL! Remote Control Denial of Service	Low	Secunia, Advisory: SA16742, September 12, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apache Software Foundation Apache 2.0.x	A vulnerability has been reported in 'modules/ssl/ssl_engine_kernel.c' because the 'ssl_hook_Access()' function does not properly enforce the 'SSLVerifyClient require' directive in a per-location context if a virtual host is configured with the 'SSLVerifyCLient optional' directive, which could let a remote malicious user bypass security policies. Patch available at: http://svn.apache.org/viewcvs?rev=264800&view=rev OpenPKG: ftp://ftp.openpkg.org/release/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ **SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** **Debian: http://security.debian.org/pool/updates/main/a/apache2/** **Mandriva: http://www.mandriva.com/security/advisories** **Slackware: ftp://ftp.slackware.com/pub/slackware/** **Trustix: http://http.trustix.org/pub/trustix/updates/** **Debian: http://security.debian.org/pool/updates/main/liba/** There is no exploit code required.	Apache 'Mod_SSL SSLVerifyClient' Restriction Bypass CAN-2005-2700	Medium	Security Tracker Alert ID: 1014833, September 1, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.017, September 3, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 Ubuntu Security Notice, USN-177-1, September 07, 2005 **SGI Security Advisory, 20050901-01-U, September 7, 2005** **Debian Security Advisory, DSA 805-1, September 8, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005** **Slackware Security Advisory, SSA:2005-251-02, September 9, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005** **Debian Security Advisory DSA 807-1, September 12, 2005** **US-CERT VU#744929**
Apple Macintosh OS X	Multiple vulnerabilities have been reported: a vulnerability was reported due to the way temporary files are handled, which could let a remote malicious user corrupt/create arbitrary files; a vulnerability was reported in the privileged helper because temporary files are created insecurely, which could let a remote malicious user corrupt/create arbitrary files; a vulnerability was reported in the Java shared	Apple Mac OS X Java Update CAN-2005-2527 CAN-2005-2528 CAN-2005-2529 CAN-2005-2530 CAN-2005-2538	Medium	Apple Security Advisory, APPLE-SA-2005-09-13, September 13, 2005

	archives update utility, which could let a malicious user obtain elevated privileges; a vulnerability was reported when using Mac OS X specific extensions due to an unspecified error, which could let a malicious user obtain elevated privileges; and a vulnerability was reported in the Java ServerSocket object because it can be created for a port that is in use, which could let a malicious user intercept traffic. Patches available at: http://www.apple.com/support/downloads/javasecurity update.html There is no exploit code required.			
Astaro Security Astaro Security Linux 6.0 01	A vulnerability has been reported due to a weakness that may allow remote malicious user to connect to arbitrary ports which could lead to access control bypass. **Upgrades available at: http://download.astaro.com/Astaro_Security_Linux/v6.0/up2date/** There is no exploit code required; however, a Proof of Concept exploit has been published.	Astaro Security Linux HTTP CONNECT Unauthorized Access CAN-2005-2729	Medium	Security Focus Bugtraq ID: 14665, August 25, 2005 **Security Focus Bugtraq ID: 14665, September 7, 2005**
BlueZ BlueZ 2.18 & prior	A vulnerability has been reported due to insufficient sanitization of input passed as a remote device name, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.bluez.org/redirect.php?url=http%3A%2F%2Fbluez.sf.net%2Fdown load%2Fbluez-libs-2.19.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200508-09.xml Debian: http://security.debian.org/pool/updates/contrib/b/bluez-utils/ Mandriva: http://www.mandriva.com/security/advisories **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.	BlueZ Arbitrary Command Execution CAN-2005-2547	High	Security Focus 14572, August 16, 2005 Gentoo Linux Security Advisory, GLSA 200508-09, August 17, 2005 Debian Security Advisory, DSA 782-1, August 23, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:150, August 25, 2005 **Conectiva Linux Announcement, CLSA-2005:1001, September 13, 2005**
common-lisp-controller common-lisp-controller	A vulnerability has been reported when validating the ownership of the cache directory, which could let a remote malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/c/common-lisp-controller/common-lisp-controller_4.15sarge2_all.deb Currently we are not aware of any exploits for this vulnerability.	Common-lisp-controller Elevated Privileges CAN-2005-2657	Medium	Debian Security Advisory, DSA 811-1, September 14, 2005
CVS CVS 1.12.7-1.12.12, 1.12.5, 1.12.2 , 1.12.1, 1.11.19, 1.11.17	A vulnerability has been reported in the 'cvsbug.in' script due to the insecure creation of temporary files, which could let a malicious user cause data loss or a Denial of Service. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Trustix: http://http.trustix.org/	CVS 'Cvsbug.In' Script Insecure Temporary File Creation CAN-2005-2693	Low	Fedora Update Notifications FEDORA-2005-790 & 791, August 23, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0045, August 26, 2005 RedHat Security Advisory, RHSA-2005:756-3,

	pub/trustix/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:20/cvsbug.patch SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ **Debian:** **http://security.debian.org/pool/updates/main/c/cvs/** **http://security.debian.org/pool/updates/main/g/gcvs/** **FreeBSD:** **ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:20.cvsbug.asc** There is no exploit code required.			September 6, 2005 SGI Security Advisory, 20050901-01-U, September 7, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:20, September 7, 2005 **Debian Security Advisories, DSA 802-1 & 806-1, September 7 & 9, 2005** **FreeBSD Security Advisory, FreeBSD-SA-05:20, September 9, 2005**
Eric Raymond Fetchmail 6.2.5	A remote buffer overflow vulnerability has been reported in the POP3 client due to insufficient boundary checks, which could let a malicious user obtain elevated privileges. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Redhat: http://rhn.redhat.com/errata/RHSA-2005-640.html Ubuntu: http://www.ubuntulinux.org/support/ documentation/usn/usn-153-1 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200507-21.xml Debian: http://security.debian.org/pool/updates/main/f/fetchmail/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.	Fetchmail POP3 Client Buffer Overflow CAN-2005-2335	Medium	Fedora Update Notifications, FEDORA-2005-613 & 614, July 21, 2005 Redhat Security Advisory, RHSA-2005:640-08, July 25, 2005 Ubuntu Security Notice, USN-153-1, July 26, 2005 Gentoo Security Advisory, GLSA 200507-21, July 25, 2005 Debian Security Advisory, DSA 774-1, August 12, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Turbolinux Security Advisory, TLSA-2005-84, August 18, 2005 **Conectiva Linux Announce-ment, CLSA-2005:1005, September 13, 2005**
GNU cpio 1.0, 1.1, 1.2	A vulnerability has been reported in 'cpio/main.c' due to a failure to create files securely, which could let a malicious user obtain sensitive information. Upgrades available at: http://ftp.gnu.org/gnu/cpio/cpio-2.6.tar.gz SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ TurboLinux:	CPIO Archiver Insecure File Creation CAN-1999-1572	Medium	Security Tracker Alert, 1013041, January 30, 2005 SGI Security Advisory, 20050204-01-U, March 7, 2005 Turbolinux Security Advisory, TLSA-2005-30, March 10, 2005 **Conectiva Linux Announcement,**

	ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** There is no exploit required.			**CLSA-2005:1002, September 13, 2005**
GNU cpio 1.0-1.3, 2.4.2, 2.5, 2.5.90, 2.6	A vulnerability has been reported when an archive is extracted into a world or group writeable directory because non-atomic procedures are used, which could let a malicious user modify file permissions. Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-378.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.32 **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-191.pdf** **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** There is no exploit code required.	CPIO CHMod File Permission Modification CAN-2005-1111	Medium	Bugtraq, 395703, April 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005:116, July 12, 2005 RedHat Security Advisory, RHSA-2005:378-17, July 21, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 SCO Security Advisory, SCOSA-2005.32, August 18, 2005 **Avaya Security Advisory, ASA-2005-191, September 6, 2005** **Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005**
GNU cpio 2.6	A Directory Traversal vulnerability has been reported when invoking cpio on a malicious archive, which could let a remote malicious user obtain sensitive information. Gentoo: http://security.gentoo.org/glsa/glsa-200506-16.xml Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.32 **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-191.pdf** **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** A Proof of Concept exploit has been published.	CPIO Directory Traversal CAN-2005-1229	Medium	Bugtraq, 396429, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200506-16, June 20, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005:116, July 12, 2005 SCO Security Advisory, SCOSA-2005.32, August 18, 2005 **Avaya Security Advisory, ASA-2005-191, September 6, 2005** **Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005**

GNU Mailutils 0.6	A format string vulnerability has been reported in 'search.c' when processing user-supplied IMAP SEARCH commands, which could let a remote malicious user execute arbitrary code. Patch available at: http://savannah.gnu.org/patch/download.php?item_id=4407&item_file_id=5 160 A Proof of Concept exploit script has been published.	GNU Mailutils Format String CAN-2005-2878	High	Security Tracker Alert ID: 1014879, September 9, 2005
IBM AIX 5.3	Buffer overflow vulnerabilities have been reported in the 'invscout,' 'paginit,' 'diagTasksWebSM,' 'getlvname,' and 'swcons' commands and multiple 'p' commands, which could let a malicious user execute arbitrary code, potentially with root privileges. IBM has released an advisory (IBM-06-10-2005) to address this and other issues. **Updated APAR availability information. Removed interim fix information.** Vendor fix available: http://www-1.ibm.com/servers/eserver/support/pseries/aixfixes.html There is no exploit code required; however, a Proof of Concept exploit has been published.	IBM AIX Multiple Buffer Overflows CAN-2005-2232 CAN-2005-2233 CAN-2005-2234 CAN-2005-2235 CAN-2005-2236 CAN-2005-2237	High	Security Tracker Alert, 1014132, June 8, 2005 IBM Security Advisory, IBM-06-10-2005, June 10, 2005 Security Focus, 13909, July 7, 2005 IBM Security Advisory, September 13, 2005
IBM AIX 5.3	A vulnerability has been reported in the NIS client which could let a remote malicious user execute arbitrary code with root privileges. **Updated APAR availability information. Removed interim fix information.** Hotfix available at: ftp://aix.software.ibm.com/aix/efixes/security/nis_2_efix.tar.Z Currently we are not aware of any exploits for this vulnerability.	IBM AIX NIS Client Remote Arbitrary Code Execution CAN-2005-1037	High	Secunia Advisory, SA14856, April 6, 2005 **IBM Security Advisory, Updated September 13, 2005**
Info-ZIP UnZip 5.52	A vulnerability has been reported due to a security weakness when extracting an archive to a world or group writable directory, which could let a malicious user modify file permissions. **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** There is no exploit code required.	Info-ZIP UnZip File Permission Modification CAN-2005-2475	Medium	Security Focus, 14450, August 2, 2005 **Fedora Update Notification, FEDORA-2005-844, September 9, 2005**
KDE KDE 3.2.0 up to including 3.4.2	A vulnerability has been reported in 'kcheckpass.c' due to the insecure creation of the lock file, which could let a malicious user obtain superuser privileges. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/post-3.4.2-kdebase-kcheckpa ss.diff Mandriva: http://www.mandriva.com/security/advisories **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/k/kdebase/** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** There is no exploit code required.	KDE kcheckpass Superuser Privilege Escalation CAN-2005-2494	High	KDE Security Advisory, September 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:160, September 6, 2005 **Ubuntu Security Notice, USN-176-1 September 07, 2005** **Slackware Security Advisory, SSA:2005-251-01, September 9, 2005**

KDE KDE 3.0 - 3.4.2	A vulnerability was reported in 'langen2kvtml' due to the insecure creation of temporary files, which could let malicious user obtain elevated privileges. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories **Slackware:** **ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/** There is no exploit code required.	KDE langen2kvtml Insecure Temporary File Creation CAN-2005-2101	Medium	KDE Security Advisory, August 15, 2005 Fedora Update Notification, FEDORA-2005-745, August 15, 2005 Fedora Update Notifications, FEDORA-2005-744 & 745, August 16, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:159, September 6, 2005 **Slackware Security Advisory, SSA:2005-251-03, September 9, 2005**
Mark D. Roth pam_per_user 0.1-0.3	A vulnerability has been reported in the authentication function due to an error when checking if the user name has been changed between calls, which could let a remote malicious user bypass authentication. Upgrades available at: ftp://ftp.feep.net/pub/software/PAM/pam_per_user/pam_per_user-0.4.tar.gz There is no exploit code required.	Mark D. Roth PAM_Per_User Authentication Bypass	Medium	Security Focus, Bugtraq ID: 14813, September 12, 2005
Mike Kershaw Kismet 2005-07-R1	Multiple vulnerabilities have been reported: an integer underflow vulnerability was reported when handling pcap files; a vulnerability was reported due to an unspecified error when handling non-printable characters in SSID; and a integer underflow vulnerability was reported in the data frame dissection, which could possibly lead to the execution of arbitrary code. Upgrade available at: http://www.kismetwireless.net/code/kismet-2005-08-R1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200508-10.xml Debian: http://security.debian.org/pool/updates/main/k/kismet/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.	Kismet Multiple Remote Vulnerabilities CAN-2005-2626 CAN-2005-2627	High	Security Focus, Bugtraq ID 14430, August 16, 2005 Gentoo Linux Security Advisory, GLSA 200508-10, August 19, 200 Debian Security Advisory, DSA 788-1, August 29, 2005 **SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005**
Multiple Vendors OpenLDAP 2.1.25; Padl Software pam_ldap Builds 166, 85, 202, 199, 198, 194, 183-192, 181, 180, 173, 172, 122, 121, 113, 107, 105	A vulnerability has been reported in OpenLDAP, 'pam_ldap,' and 'nss_ldap' when a connection to a slave is established using TLS and the client is referred to a master, which could let a remote malicious user obtain sensitive information. Trustix: http://http.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-13.xml Mandriva: http://www.mandriva.com/	Multiple Vendors TLS Plaintext Password CAN-2005-2069	Medium	Trustix Secure Linux Advisory, TSLSA-2005-0031, July 1, 2005 Gentoo Linux Security Advisory, GLSA 200507-13, July 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:121, July 19, 2005 Ubuntu Security Notice,

security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/libn/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.		USN-152-1, July 21, 2005 Turbolinux Security Advisory, TLSA-2005-86 & 87, August 29, 2006 **SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005**

Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3 , 0.1-0.1.6 1, 0.0.1-0.0.6	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: ftp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml SUSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ Mandriva: http://www.mandriva.com/security/advisories OpenBSD: http://www.openbsd.org/errata.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ zsync: http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download Apple: http://docs.info.apple.com/article.html?artnum=302163 SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id = 35093&release_id=351848 Debian: http://security.debian.org/	Zlib Compression Library Buffer Overflow CAN-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005 Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 USCERT Vulnerability Note VU#680620, July 22, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Security Focus, Bugtraq ID: 14162, August 26, 2005 Debian Security Advisory, DSA 797-1, September 1,

	pool/updates/main/z/zsync/ **Trolltech:** **ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz** Currently we are not aware of any exploits for this vulnerability.			2005 **Security Focus, Bugtraq ID: 14162, September 12, 2005**
Multiple Vendors zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input. Zlib: http://www.zlib.net/zlib-1.2.3.tar.gz Debian: http://security.debian.org/pool/updates/main/z/zlib/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ OpenBSD: http://www.openbsd.org/errata.html#libz2 Mandriva: http://www.mandriva.com/security/ advisories?name=MDKSA-2005:124 Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.323596 FreeBSD: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc SUSE: http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html Gentoo: http://security.gentoo.org/glsa/glsa-200507-28.xml http://security.gentoo.org/glsa/glsa-200508-01.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Apple: http://docs.info.apple.com/article.html?artnum=302163 TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CAN-2005-1849	Low	Security Focus, Bugtraq ID 14340, July 21, 2005 Debian Security Advisory DSA 763-1, July 21, 2005 Ubuntu Security Notice, USN-151-1, July 21, 2005 OpenBSD, Release Errata 3.7, July 21, 2005 Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005 Secunia, Advisory: SA16195, July 25, 2005 Slackware Security Advisory, SSA:2005-203-03, July 22, 2005 FreeBSD Security Advisory, SA-05:18, July 27, 2005 SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005 Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005 Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005 Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005 Turbolinux Security Advisory , TLSA-2005-83, August 18, 2005 SCO Security Advisory, SCOSA-2005.33, August 19, 2005 Debian Security Advisory, DSA 797-1, September 1, 2005 **Security Focus, Bugtraq ID: 14340, September 12, 2005**

	SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33 Debian: http://security.debian.org/pool/updates/main/z/zsync/ **Trolltech:** **ftp://ftp.trolltech.com/qt/source/qt-x11-free-3.3.5.tar.gz** Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors dhcpcd 1.3.22	A vulnerability has been reported in dhcpcd that could let a remote user perform a Denial of Service. Debian: http://security.debian.org/pool/updates/main/d/dhcpcd/ Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200507-16.xml Conectiva: http://distro.conectiva.com.br/atualizacoes/ index.php?id=a&anuncio=000983 RedHat: http://rhn.redhat.com/errata/RHSA-2005-603.html Debian: http://security.debian.org/pool/updates/main/ IPCop: http://sourceforge.net/project/showfiles.php?group_id=40604&package_id =35093&release_id=351848 **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** Currently we are not aware of any exploits for this vulnerability.	dhcpcd Denial of Service CAN-2005-1848	Low	Secunia, Advisory: SA15982, July 11, 2005 Debian Security Advisory, DSA 750-1, July 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:117, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-16, July 15, 2005 Conectiva, CLSA-2005:983, July 25, 2005 RedHat Security Advisory, RHSA-2005:603-07, July 27, 2005 Debian Security Advisor, DSA 773-1, August 11, 2005 Security Focus, Bugtraq ID: 14206 , August 26, 2005 **Slackware Security Advisory, SSA:2005-255-01, September 12, 2005**
Multiple Vendors Gentoo Linux; RedHat Fedora Core3, Core2; SUSE Linux 8.1, 8.2, 9.0-9.2, Desktop 1.0, Enterprise Server 9, 8, Novell Linux Desktop 1.0; X.org X11R6 6.7 .0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0-4.0.3, 4.1 .0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1 4.3 .0	Multiple vulnerabilities exist due to integer overflows, memory access errors, input validation errors, and logic errors, which could let a remote malicious user execute arbitrary code, obtain sensitive information, or cause a Denial of Service. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates Gentoo: http://security.gentoo.org/glsa/glsa-200411-28.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE X.org: http://www.x.org/pub/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/	Multiple Vendors LibXPM Multiple Vulnerabilities CAN-2004-0914	High	X.Org Foundation Security Advisory, November 17, 2004 Fedora Update Notifications, FEDORA-2004-433 & 434, November 17 & 18, 2004 SUSE Security Announcement, SUSE-SA:2004:041, November 17, 2004 Gentoo Linux Security Advisory, GLSA 200411-28, November 19, 2004 Fedora Security Update Notifications FEDORA-2003-464, 465, 466, & 467, December 1, 2004 RedHat Security Advisory,

core/updates/2/

RedHat:
http://rhn.redhat.com/errata/RHSA-2004-537.html

Mandrakesoft:
http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:137
(libxpm)

http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:138
(XFree86)

Debian:
http://www.debian.org/security/2004/dsa-607
(XFree86)

SGI:
ftp://patches.sgi.com/support/free/security/patches/ProPack/3/

TurboLinux:
http://www.turbolinux.com/update/

Avaya:
http://support.avaya.com/elmodocs2/security/ASA-2005-023_RHSA-2004-537.pdf

http://support.avaya.com/elmodocs2/security/ASA-2005-025_RHSA-2005-004.pdf

Gentoo:
http://security.gentoo.org/glsa/glsa-200502-06.xml

http://security.gentoo.org/glsa/glsa-200502-07.xml

Ubuntu:
http://security.ubuntu.com/ubuntu/pool/

FedoraLegacy:
http://download.fedoralegacy.org/redhat/

Ubuntu:
http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/

Currently we are not aware of any exploits for these vulnerabilities.

RHSA-2004:537-17, December 2, 2004

Mandrakesoft:
MDKSA-2004:137: libxpm4;
MDKSA-2004:138: XFree86, November 22, 2004

Debian Security Advisory DSA-607-1 xfree86 -- several vulnerabilities, December 10, 2004

Turbolinux Security Announcement, January 20, 2005

Avaya Security Advisories, ASA-2005-023 & 025, January 25, 2005

Gentoo Linux Security Advisories, GLSA 200502-06 & 07, February 7, 2005

Ubuntu Security Notice, USN-83-1 February 16, 2005

Fedora Legacy Update Advisory, FLSA:2314, March 2, 2005

Ubuntu Security Notice, USN-83-2, September 12, 2005

Multiple Vendors IPsec-Tools IPsec-Tools 0.5; KAME Racoon prior to 20050307	A remote Denial of Service vulnerability has been reported when parsing ISAKMP headers. Upgrades available at: http://www.kame.net/snap-users/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-232.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/i/ipsec-tools/ **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.37** Currently we are not aware of any exploits for this vulnerability.	KAME Racoon Malformed ISAKMP Packet Headers Remote Denial of Service CAN-2005-0398	Low	Fedora Update Notifications, FEDORA-2005-216 & 217, March 14, 2005 RedHat Security Advisory, RHSA-2005:232-10, March 23, 2005 Gentoo Linux Security Advisory, GLSA 200503-33, March 25, 2005 ALTLinux Security Advisory, March 29, 2005 SUSE Security Announcement, SUSE-SA:2005:020, March 31, 2005 Ubuntu Security Notice, USN-107-1, April 05, 2005 **SCO Security Advisory, SCOSA-2005.37, September 9, 2005**
Multiple Vendors Linux kernel 2.6 prior to 2.6.12.1	A Denial of Service vulnerability has been reported in the subthread exec signal processing that has a timer pending. Updates available at: http://www.kernel.org/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Subthread Exec Denial of Service CAN-2005-1913	Low	Security Tracker Alert ID: 1014274, June 23, 2005 **Ubuntu Security Notice, USN-178-1, September 09, 2005**
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A vulnerability has been reported in the EXT2/EXT3 file systems, which could let a remote malicious user bypass access controls. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel EXT2/EXT3 File Access Bypass CAN-2005-2801	Medium	Security Focus, Bugtraq ID: 14792, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005
Multiple Vendors Linux kernel 2.6.8, 2.6.10	A remote Denial of Service vulnerability has been reported in the 'ipt_recent' module when specially crafted packets are sent. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'Ipt_recent' Remote Denial of Service CAN-2005-2872	Low	Security Focus, Bugtraq ID: 14791, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005

Multiple Vendors Linux kernel 2.6.8-2.6.10, 2.4.21	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'msg_control' when copying 32 bit contents, which could let a malicious user obtain root privileges and execute arbitrary code; and a vulnerability was reported in the 'raw_sendmsg()' function, which could let a malicious user obtain sensitive information or cause a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service CAN-2005-2490 CAN-2005-2492	High	Secunia Advisory: SA16747, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005
Multiple Vendors RedHat Fedora Core3, Enterprise Linux ES 4, ES 3, AS 4, AS 3; FreeRADIUS 1.0.4	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'exec.c' due to a boundary error when handling 'radius_exec_program()' function environment variables, which could let a remote malicious user cause a Denial of Service; a vulnerability was reported in 'token.c' and 'sql_unixodbc.c' due to off-by-one errors, which could let a remote malicious user cause a Denial of Service; a vulnerability was reported in 'xlat.c' due to a boundary error when handling server replies; and a vulnerability was reported in 'rlm_ldap.c' due to an error when escaping ldap data, which could let a remote malicious user obtain sensitive information. Upgrades available at: ftp://ftp.freeradius.org/pub/radius/freeradius-1.0.5.tar.gz Currently we are not aware of any exploits for these vulnerabilities.	FreeRADIUS Multiple Remote Vulnerabilities	Medium	Secunia Advisory: SA16712, September 8, 2005
Multiple Vendors SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, 9.0, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, 9.0, x86_64; KAudioCreator	A vulnerability has been reported in the CDDB entry title due to insufficient sanitization of user-supplied input, which could let a remote malicious user overwrite arbitrary files. SUSE: ftp://ftp.suse.com/pub/suse/ There is no exploit code required.	KAudioCreator CDDB Arbitrary File Overwrite	Medium	SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Rob Flynn Gaim 1.3.1, 1.3 .0, 1.2.1, 1.2 , 1.1.1 -1.1.4, 1.0-1.0.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Desktop 4.0, Advanced Workstation for the Itanium Processor 2.1, IA64	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported due to the way away messages are handled, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability has been reported due to an error when handling file transfers. Updates available at: http://gaim.sourceforge.net/downloads.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-589.html http://rhn.redhat.com/errata/RHSA-2005-627.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-06.xml SGI: ftp://patches.sgi.com/support/free/security/advisories/ Mandriva: http://www.mandriva.com/security/advisories	Gaim AIM/ICQ Protocols Buffer Overflow & Denial of Service CAN-2005-2102 CAN-2005-2103	High	RedHat Security Advisories, RHSA-2005:589-16 & RHSA-2005:627-11, August 9, 2005 Ubuntu Security Notice, USN-168-1, August 12, 2005 Gentoo Linux Security Advisory, GLSA 200508-06, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:139, August 16, 2005 Fedora Update Notifications, FEDORA-2005-750 & 751, August 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 Slackware Security Advisory, SSA:2005-242-03, August

	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **SUSE:** **ftp://ftp.suse.com/pub/suse/** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** A Proof of Concept exploit has been published for the buffer overflow vulnerability.			31, 2005 **Slackware Security Advisory, SSA:2005-251-03, September 9, 2005** **SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005** **Conectiva Linux Announcement, CLSA-2005:1006, September 13, 2005**
Multiple Vendors Glyph and Cog Xpdf 3.0, pl2 & pl3; Ubuntu Linux 5.0 4 powerpc, i386, amd64; RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0; KDE 3.4.1, 3.4, 3.3.1, 3.3.2; GNOME GPdf 2.8.3, 2.1	A remote Denial of Service vulnerability has been reported when verifying malformed 'loca' table in PDF files. RedHat: http://rhn.redhat.com/errata/RHSA-2005-670.html http://rhn.redhat.com/errata/RHSA-2005-671.html http://rhn.redhat.com/errata/RHSA-2005-708.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xpdf/ KDE: http://www.kde.org/info/security/advisory-20050809-1.txt Mandriva: http://www.mandriva.com/security/advisories SGI: ftp://patches.sgi.com/support/free/security/advisories/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-08.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/k/kdegraphics/ Trustix: http://http.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.	XPDF Loca Table Verification Remote Denial of Service CAN-2005-2097	Low	RedHat Security Advisories, RHSA-2005:670-05 & RHSA-2005:671-03, & RHSA-2005:708-05, August 9, 2005 Ubuntu Security Notice, USN-163-1, August 09, 2005 KDE Security Advisory, 20050809-1, August 9, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:134, 135, 136 & 138, August 11, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Gentoo Linux Security Advisory GLSA, 200508-08, August 16, 2005 Fedora Update Notifications, FEDORA-2005-729, 730, 732, & 733, August 15 & 17, 2005 Debian Security Advisory, DSA 780-1, August 22, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005 Turbolinux Security Advisory, TLSA-2005-88, September 5, 2005 **Conectiva Linux Announce-ment, CLSA-2005:1010, September 13, 2005**

Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; GNOME Evolution 2.3.1 -2.3.6 .1, 2,0- 2.2 , 1.5	Multiple format string vulnerabilities have been reported: a vulnerability was reported when vCard information is attached to an email message, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when specially crafted contact data that has been retrieved from an LDAP server is displayed, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported when specially crafted task list data that has been retrieved from remote servers and the data has been saved under the 'Calendars' tab is displayed, which could let a remote malicious user execute arbitrary code. Updates available at: http://ftp.gnome.org/pub/gnome/sources/evolution/2.3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/evolution/ Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-12.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-267.html **SGI:** **ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for these vulnerabilities.	GNOME Evolution Multiple Format String CAN-2005-2549 CAN-2005-2550	High	Secunia Advisory: SA16394, August 11, 2005 Ubuntu Security Notice, USN-166-1, August 11, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:141, August 18, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 Gentoo Linux Security Advisory, GLSA 200508-12, August 23, 200 RedHat Security Advisory, RHSA-2005:267-10, August 29, 2005 **SGI Security Advisory, 20050901-01-U, September 7, 2005** **Conectiva Linux Announce-ment, CLSA-2005:1004, September 13, 2005**
Multiple Vendors Ubuntu Linux 5.0 4, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6-2.6.13	A Denial of Service vulnerability has been reported in the '/proc/scsi/sg/devices' file due to a memory leak. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ A Proof of Concept exploit has been published.	Linux Kernel SCSI ProcFS Denial of Service CAN-2005-2800	Low	Security Focus, Bugtraq ID: 14790, September 9, 2005 Ubuntu Security Notice, USN-178-1, September 09, 2005
Multiple Vendors util-linux 2.8-2.13; Andries Brouwer util-linux 2.11 d, f, h, i, k, l, n, u, 2.10 s	A vulnerability has been because mounted filesystem options are improperly cleared due to a design flaw, which could let a remote malicious user obtain elevated privileges. Updates available at: http://www.kernel.org/pub/linux/utils/util-linux/testing/util-linux-2.12r-pre1.tar.gz Slackware: ftp://ftp.slackware.com/pub/slackware/ There is no exploit code required.	Util-Linux UMount Remounting Filesystem Elevated Privileges CAN-2005-2876	Medium	Security Focus, Bugtraq ID: 14816, September 12, 2005 Slackware Security Advisory, SSA:2005-255-02, September 13, 2005

Multiple Vendors XFree86 X11R6 4.3 .0, 4.1 .0; X.org X11R6 6.8.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Advanced Workstation for the Itanium Processor 2.1, IA64; Gentoo Linux	A buffer overflow vulnerability has been reported in the pixmap processing code, which could let a malicious user execute arbitrary code and possibly obtain superuser privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200509-07.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-329.html http://rhn.redhat.com/errata/RHSA-2005-396.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ Mandriva: http://www.mandriva.com/security/advisories?name=MDKSA-2005:164 Currently we are not aware of any exploits for this vulnerability.	XFree86 Pixmap Allocation Buffer Overflow CAN-2005-2495	High	Gentoo Linux Security Advisory, GLSA 200509-07, September 12, 2005 RedHat Security Advisory, RHSA-2005:329-12 & RHSA-2005:396-9, September 12 & 13, 2005 Ubuntu Security Notice, USN-182-1, September 12, 2005 Mandriva Security Advisory, MDKSA-2005:164, September 13, 2005 US-CERT VU#102441
netpbm 10.0	A vulnerability has been reported in netpbm ('-dSAFER') that could let malicious users execute arbitrary postscript code. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-04.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-743.html **SGI:** **ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** There is no exploit code required.	netpbm Arbitrary Code Execution CAN-2005-2471	High	Secunia Advisory: SA16184, July 25, 2005 Trustix Secure Linux Security Advisory, #2005-0038, July 29, 2005 Gentoo Linux Security Advisory, GLSA 200508-04, August 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:133, August 10, 2005 Ubuntu Security Notice, USN-164-1, August 11, 2005 Fedora Update Notifications, FEDORA-2005-727 & 728, August 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 RedHat Security Advisory, RHSA-2005:743-08, August 22, 2005 **SGI Security Advisory, 20050901-01-U, September 7, 2005**
Open Webmail Open Webmail 2.41	A Cross-Site Scripting vulnerability has been reported in 'openwebmail-main.pl' due to insufficient sanitization of the 'sessionid' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Open WebMail Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 14771, September 7, 2005
PCRE PCRE 6.1, 6.0, 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available at: http://www.pcre.org/	PCRE Regular Expression Heap Overflow CAN-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005 Ubuntu Security Notices,

	Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/pcre3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-17.xml Mandriva: http://www.mandriva.com/security/advisories SUSE: ftp://ftp.SUSE.com/pub/SUSE Slackware: ftp://ftp.slackware.com/pub/slackware/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/ Debian: http://security.debian.org/pool/updates/main/p/pcre3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE **Slackware:** **ftp://ftp.slackware.com/pub/slackware/slackware-10.1/testing/packages/php-5.0.5/php-5.0.5-i486-1.tgz** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200509-08.xml** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for this vulnerability.			USN-173-1 & 173-2, August 24, 2005 Fedora Update Notifications, FEDORA-2005-802 & 803, August 24, 2005 Gentoo Linux Security Advisory, GLSA 200508-17, August 25, 2005 Mandriva Linux Security Update Advisories, MDKSA-2005:151-155, August 25, 26, & 29, 2005 SUSE Security Announcements, SUSE-SA:2005:048 & 049, August 30, 2005 Slackware Security Advisories, SSA:2005-242-01 & 242-02 , August 31, 2005 Ubuntu Security Notices, USN-173-3, 173-4 August 30 & 31, 2005 Debian Security Advisory, DSA 800-1, September 2, 2005 SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005 **Slackware Security Advisory, SSA:2005-251-04, September 9, 2005** **Gentoo Linux Security Advisory, GLSA 200509-08, September 12, 2005** **Conectiva Linux Announce-ment, CLSA-2005:1009, September 13, 2005**
Snort Project Snort 2.4 .0, 2.3.0-2.3.3, 2.2, 2.1.3, 2.1.1 RC1, 2.1 .0, 2.0.6, 2.0.4, 2.0 rc2, 2.0 .0rc1, 2.0	A remote Denial of Service vulnerability has been reported in 'log.c' in the 'PrintTcpOptions()' function due to a failure to handle malicious TCP packets. No workaround or patch available at time of publishing. An exploit script has been published.	Snort 'PrintTcpOptions' Remote Denial of Service	Low	Snort Advisory, September 12, 2005
Squid Web Proxy Squid Web Proxy Cache 2.5 & prior	A remote Denial of Service vulnerability has been reported in the 'storeBuffer()' function when handling aborted requests. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE10-STORE_PENDING.patch Gentoo: http://security.gentoo.org/glsa/glsa-200509-06.xml	Squid Aborted Requests Remote Denial of Service CAN-2005-2794	Low	Security Tracker Alert ID: 1014864, September 7, 2005 Gentoo Linux Security Advisory GLSA 200509-06, September 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.021, September 10, 2005 Mandriva Linux Security

	OpenPKG: ftp://ftp.openpkg.org/release/ Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/s/squid/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/s/squid/ Currently we are not aware of any exploits for this vulnerability.			Update Advisory, MDKSA-2005:162, September 12, 2004 Debian Security Advisory, DSA 809-1, September 13, 2005 Ubuntu Security Notice, USN-183-1, September 13, 2005
Squid Web Proxy Squid Web Proxy Cache 2.5 .STABLE1-STABLE 10, 2.4 .STABLE6 & 7, STABLE 2, 2.4, 2.3 STABLE 4&5, 2.1 Patch 2, 2.0 Patch 2	A remote Denial of Service vulnerability has been reported in '/squid/src/ssl.c' when a malicious user triggers a segmentation fault in the 'sslConnectTimeout()' function. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE10-sslConnectTimeout.patch **Trustix:** **http://http.trustix.org/pub/trustix/updates/** **OpenPKG:** **ftp://ftp.openpkg.org/release/** **Mandriva:** **http://www.mandriva.com/security/advisories** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/s/squid/** **Debian:** **http://security.debian.org/pool/updates/main/s/squid/** There is no exploit code required.	Squid 'sslConnect Timeout()' Remote Denial of Service CAN-2005-2796	Low	Security Tracker Alert ID: 1014846, September 2, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005** **OpenPKG Security Advisory, OpenPKG-SA-2005.021, September 10, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:162, September 12, 2005** **Ubuntu Security Notice, USN-183-1, September 13, 2005** **Debian Security Advisory, DSA 809-1, September 13, 2005**
TMSNC TMSNC 0.2.4	A format string vulnerability has been reported in 'ur.c' when the 'wprintw()' function is used, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://prdownloads.sourceforge.net/tmsnc/tmsnc-0.2.5.tar.gz?download Currently we are not aware of any exploits for this vulnerability.	TMSNC Format String	High	Security Focus Bugtraq ID: 14810, September 12, 2005

Vim V6.3.082	A vulnerability has been reported in Vim that could let remote malicious users execute arbitrary code. Vendor patch available: ftp://ftp.vim.org/pub/vim/patches/6.3/6.3.082 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/v/vim/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-745.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-189.pdf **SGI:** **ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** There is no exploit code required; however, Proof of Concept exploits have been published.	Vim Arbitrary Code Execution CAN-2005-2368	High	Security Focus, 14374, July 25, 2005 Ubuntu Security Notice, USN-154-1, July 26, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0038, July 29, 2005 Fedora Update Notifications, FEDORA-2005-737, 738, & 741, August 10 & 15, 2005 Conectiva Security Advisory, CLSA-2005:995, Mandriva Linux Security Update Advisory, MDKSA-2005:148, August 22, 2005 RedHat Security, Advisory, RHSA-2005:745-10, August 22, 2005 Avaya Security Advisory, ASA-2005-189-, August 31, 2005 **SGI Security Advisory, 20050901-01-U, September 7, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apache	A vulnerability has been reported in Apache which can be exploited by remote malicious users to smuggle http requests. Conectiva: http://distro.conectiva.com.br/ atualizacoes/index.php?id=a&anuncio=000982 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SGI:	Apache HTTP Request Smuggling Vulnerability CAN-2005-1268 CAN-2005-2088	Medium	Secunia, Advisory: SA14530, July 26, 2005 Conectiva, CLSA-2005:982, July 25, 2005 Fedora Update Notification FEDORA-2005-638 & 639, August 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:129, August 3, 2005 Ubuntu Security Notice, USN-160-1, August 04, 2005 Turbolinux Security Advisory, TLSA-2005-81, August 9, 2005 SGI Security Advisory, 20050802-01-U, August

	ftp://patches.sgi.com/support/free/security/advisories/ SuSE: ftp://ftp.suse.com/pub/suse/ **Debian:** **http://security.debian.org/pool/updates/main/a/apache/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/a/apache/** **SGI:** **ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** Currently we are not aware of any exploits for this vulnerability.			15, 2005 SUSE Security Announcement, SUSE-SA:2005:046, August 16, 2005 **Debian Security Advisory DSA 803-1, September 8, 2005** **Ubuntu Security Notice, USN-160-2, September 07, 2005** **SGI Security Advisory, 20050901-01-U, September 7, 2005**
ARTC ATutor 1.5.1	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'Password_Reminder.php' due to insufficient sanitation before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported due to insufficient access validation before granting access to privileged information, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	ATutor 'Password_Reminder.PHP' SQL Injection & Information Disclosure	Medium	Security Focus, Bugtraq IDs: 14831 & 14832, September 14, 2005
Azerbaijan Development Group AzDGDatingLite 2.1.3	A Directory Traversal vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user include arbitrary files. No workaround or patch available at time of publishing. There is no exploit code required; however, an exploit script has been published.	Azerbaijan Development Group AZDGDatingLite Directory Traversal	Medium	Security Focus, Bugtraq ID: 14819, September 13, 2005
CGI Central aMember Pro 2.3.4	A vulnerability has been reported due to insufficient sanitization of various scripts, which could let a remote malicious user execute arbitrary server-side script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	AMember Remote File Include	Medium	Security Focus, Bugtraq ID: 14777, September 8, 2005
Check Point Software SecurePlatform NGX R60 Build 244	A vulnerability has been reported due to improper implementation of expected firewall rules, which could let a remote malicious user bypass firewall rules. No workaround or patch available at time of publishing. There is no exploit code required.	Check Point SecurePlatform NGX Firewall Rules Bypass CAN-2005-2889	Medium	Security Focus, Bugtraq ID: 14781, September r8, 2005
Cisco Systems CSS11501 Content Services Switch, CSS11500 Content Services Switch	A vulnerability has been reported when SSL encryption is enabled and client authentication using SSL certificates is enabled due to a failure to properly renegotiate the SSL session, which could let a remote malicious user bypass security restrictions. Patch information available at: http://www.cisco.com/warp/public/707/cisco-sn-20050908-css.shtml Currently we are not aware of any exploits for this vulnerability.	Cisco CSS 11500 Series SSL Authentication Bypass	Medium	Cisco Security Notice: Document ID: 66280, September 8, 2005

class-1 class-1 forum 0.24.4	An SQL injection vulnerability has been reported which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Class-1 Forum SQL Injection CAN-2005-2902	Medium	Security Focus, Bugtraq ID: 14774, September 8, 2005
CrashCool.com PhpTagCool 1.0.3	An SQL injection vulnerability was reported in the 'X-Forwarded-For' HTTP header due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, an exploit script has been published.	PhpTagCool SQL Injection	Medium	Security Tracker Alert ID: 1014878, September 9, 2005
Distributed Checksum ClearingHouse DCC 1.3-1.3.15	A remote Denial of Service vulnerability has been reported in 'dccifd' when an email message is received that doesn't contain a message body. Upgrades available at: http://www.rhyolite.com/anti-spam/dcc/source/dcc.tar.Z There is no exploit code required.	Distributed Checksum ClearingHouse DCCIFD Denial of Service	Low	Security Focus Bugtraq ID: 14769, September 7, 2005
Ethereal Ethereal V0.10.11	Multiple dissector and zlib vulnerabilities have been reported in Ethereal that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version 0.10.12: http://www.ethereal.com/download.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-687.html SUSE: ftp://ftp.suse.com/pub/suse/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-185.pdf **SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** **Conectiva: ftp://atualizacoes.conectiva.com.br/10/** Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Denial of Service or Arbitrary Code Execution CAN-2005-2361 CAN-2005-2362 CAN-2005-2363 CAN-2005-2364 CAN-2005-2365 CAN-2005-2366 CAN-2005-2367	High	Secunia, Advisory: SA16225, July 27, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:131, August 4, 2005 RedHat Security Advisory, RHSA-2005:687-03, August 10, 2005 SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005 Avaya Security Advisory, ASA-2005-185, August 30, 2005 **SGI Security Advisory, 20050901-01-U, September 7, 2005** **Conectiva Linux Announce-ment, CLSA-2005:1003, September 13, 2005**
Flowerfire Sawmill 7.1.13	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Updates available at: http://www.sawmill.net/us_downloads.html There is no exploit code required.	Sawmill Cross-Site Scripting	Medium	Secunia Advisory: SA16744, September 9, 2005

Hewlett Packard Company OpenView Network Node Manager 7.50 Solaris, 7.50, 6.41 Solaris, 6.41	A vulnerability has been reported in the 'node' URI parameter of the 'OvCgi/connectedNodes.ovpl' script, which could let a remote malicious user execute arbitrary code. **Revision 3:** **Added PHSS_33783.** **Added preliminary files for OV NNM 7.01, 6.4, 6.2** Workaround available at: http://support.openview.hp.com/news_archives.jsp There is no exploit code required; however, a Proof of Concept exploit script has been published.	HP OpenView Network Node Manager Remote Arbitrary Code Execution CAN-2005-2773	High	Portcullis Security Advisory, 05-014, August 25, 2005 HP Security Advisory, HPSBMA01224, August 26, 2005 **HP Security Advisory, HPSBMA01224 REVISION: 3, September 13, 2005**
IBM OS/400 V5R1M0	Several vulnerabilities have been reported: a vulnerability was reported because the local CA (Certificate Authority) certificates do not contain the X509 basic constraints extension, which could lead to incorrect verification of certification chains; a vulnerability was reported due to an error in the certificate store because an old certificate associated with an application identifier can be returned even when it has been renewed; and a vulnerability was reported in ASN.1 parsing due to an unspecified error. PTFs are reportedly available, which fix these security issues. Currently we are not aware of any exploits for these vulnerabilities.	IBM OS/400 Multiple OSP-CERT Vulnerabilities	Medium	Secunia Advisory: SA16751, September 9, 2005
IBM OS/400 V5R1M0	A remote Denial of Service vulnerability has been reported due to an error when handling certain malformed SNMP messages. A PTF is reportedly available, which fixes the vulnerability. There is no exploit code required.	IBM OS/400 Malformed SNMP Requests Remote Denial of Service	Low	Secunia Advisory: SA16735, September 9, 2005
Ingate Systems Ingate SIParator 4.2.1-4.2.3 , Firewall 4.2.1-4.2.3	A Cross-Site Scripting vulnerability has been reported in the administrative interface due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code. The vendor has reported that this vulnerability will be fixed in an upcoming release. There is no exploit code required.	Ingate Administrative Interface Cross-Site Scripting	Medium	Secunia Advisory: SA16776, September 12, 2005
KDE KDE 3.4, 3.3-3.3.2, 3.2-3.2.3	A vulnerability has been reported in KDE Kate and KWrite because backup files are created with default permissions even if the original file had more restrictive permissions set, which could let a local/remote malicious user obtain sensitive information. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-612.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **Debian:** **http://security.debian.org/pool/updates/main/k/kdelibs/** There is no exploit code required.	KDE Kate, KWrite Local Backup File Information Disclosure CAN-2005-1920	Medium	Security Tracker Alert ID: 1014512, July 18, 2005 Fedora Update Notification, FEDORA-2005-594, July 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:122, July 20, 2005 RedHat Security Advisory, RHSA-2005:612-07, July 27, 2005 Conectiva Linux Announcement, CLSA-2005:988, August 4, 2005 **Debian Security Advisory, DSA 804-1, September 8, 2005**
Linksys WRT54G v4.0 4.20.6 (Firmware), v4.0 4.0.7 (Firmware), v3.0 3.3.6 (Firmware), v3.0 3.1.3 (Firmware), v2.0 2.4.4 (Firmware)	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'POST' method handlers when handling a negative 'Content-Length' value, which could let a remote malicious user cause a Denial of Service; a vulnerability was reported in 'upgrade.cgi' due to a design error, which could let a remote unauthenticated malicious user upload arbitrary firmware; a vulnerability was reported in 'restore.cgi' due to a design error, which could let a remote unauthenticated malicious user upload arbitrary configuration settings; a vulnerability was reported in 'apply.cgi' due to a boundary error when a POST request is submitted that contains a content length longer than 10000 bytes, which could let a remote malicious user cause a Denial of Service	Linksys WRT54G Wireless Router Multiple Remote Vulnerabilities CAN-2005-2912 CAN-2005-2913 CAN-2005-2914 CAN-2005-2915 CAN-2005-2916	High	iDEFENSE Security Advisory, September 13, 2005

	and possibly execute arbitrary code with ROOT privileges; and a vulnerability was reported in 'ezconfig.asp' due to an authentication error, which could let a remote unauthenticated malicious user upload configuration settings to a vulnerable device if the fixed 256-byte XOR key used to encrypt the settings is known. No workaround or patch available at time of publishing. There is no exploit code required for most of these vulnerabilities.			
Mimicboard2 Mimicboard2 086	Multiple HTML injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'mimic2.dat' due to insufficient user authentication, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	Mimicboard2 Multiple HTML Injection & Unauthorized Access	Medium	Exploit Labs Advisory, EXPL-A-2005-013, September 8, 2005
Miva Corporation Miva Merchant 5.0	A Cross-Site Scripting vulnerability has been reported in 'Merchant.MVC' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Update available at: http://smallbusiness.miva.com/products/merchant/ There is no exploit code required; however, a Proof of Concept exploit has been published.	MIVA Merchant 5 Cross-Site Scripting	Medium	Security Focus, Bugtraq ID: 14828, September 14, 2005
Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'InstallTrigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/ Gentoo: ftp://security.gentoo.org/glsa/ Mandriva: http://www.mandriva.com/security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/	Firefox Multiple Vulnerabilities CAN-2005-2260 CAN-2005-2261 CAN-2005-2262 CAN-2005-2263 CAN-2005-2264 CAN-2005-2265 CAN-2005-2267 CAN-2005-2269 CAN-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005 RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July 22, 2005 US-CERT VU#652366 US-CERT VU#996798 Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 SUSE Security Announcement, SUSE-SA:2005:045,

	errata/RHSA-2005-586.html Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/epiphany-browser/ http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ http://security.debian.org/pool/updates/main/m/mozilla/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Gentoo: http://security.gentoo.org/glsa/glsa-200507-24.xml Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/m/mozilla-firefox/ **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla/** Exploits have been published.			August 11, 2005 Debian Security Advisory, DSA 775-1, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Debian Security Advisory, DSA 777-1, August 17, 2005 Debian Security Advisory, DSA 779-1, August 20, 2005 Debian Security Advisory, DSA 781-1, August 23, 2005 Gentoo Linux Security Advisory, GLSA 200507-24, August 26, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:127-1, August 26, 2005 Slackware Security Advisory, SSA:2005-085-01, August 28, 2005 Debian Security Advisory, DSA 779-2, September 1, 2005 **Debian Security Advisory, DSA 810-1, September 13, 2005**
Mozilla.org Netscape 8.0.3.3, 7.2; Mozilla Firefox 1.5 Beta1, 1.0.6, Mozilla Browser 1.7.11	A buffer overflow vulnerability has been reported due to an error when handling IDN URLs that contain the 0xAD character in the domain name, which could let a remote malicious user execute arbitrary code. Patches available at: http://ftp.mozilla.org/pub/mozilla.org/firefox/releases/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-769.html http://rhn.redhat.com/errata/RHSA-2005-768.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu:	Mozilla/Netscape/ Firefox Browsers Domain Name Buffer Overflow CAN-2005-2871	High	Security Focus, Bugtraq ID: 14784, September 10, 2005 RedHat Security Advisories, 769-8 & RHSA-2005:768-6, September 9,2005 Fedora Update Notifications, FEDORA-2005-871-184, September 10, 2005 Ubuntu Security Notice, USN-181-1, September 12, 2005 US-CERT VU#573857

	http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ A Proof of Concept exploit script has been published.			
Multiple Vendors Gentoo Linux; Apache Software Foundation Apache 2.1-2.1.5, 2.0.35-2.0.54, 2.0.32, 2.0.28, Beta, 2.0 a9, 2.0	A remote Denial of Service vulnerability has been reported in the HTTP 'Range' header due to an error in the byte-range filter. Patches available at: http://issues.apache.org/bugzilla/attachment.cgi?id=16102 Gentoo: http://security.gentoo.org/glsa/glsa-200508-15.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-608.html **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/a/apache2/** **Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/** **Debian: http://security.debian.org/pool/updates/main/a/apache2/** **Trustix: http://http.trustix.org/pub/trustix/updates/** **Mandriva: http://www.mandriva.com/security/advisories** **SUSE: ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	Apache Remote Denial of Service CAN-2005-2728	Low	Secunia Advisory: SA16559, August 25, 2005 Security Advisory, GLSA 200508-15, August 25, 2005 RedHat Security Advisory, RHSA-2005:608-7, September 6, 2005 **Ubuntu Security Notice, USN-177-1, September 07, 2005** **Fedora Update Notifications, FEDORA-2005-848 & 849, September 7, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:161, September 8, 2005** **SGI Security Advisory, 20050901-01-U, September 7, 2005** **Debian Security Advisory, DSA 805-1, September 8, 2005** **Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005** **SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005**

Multiple Vendors PHPXMLRPC 1.1.1; PEAR XML_RPC 1.3.3; Drupal 4.6-4.6.2, 4.5-4.5.4; Nucleus CMS Nucleus CMS 3.21, 3.2, 3.1, 3.0, RC, 3.0.; MailWatch for MailScanner 1.0.1; eGroupWare 1.0.6, 1.0.3, 1.0.1, 1.0.0.007, 1.0	A vulnerability has been reported in XML-RPC due to insufficient sanitization of certain XML tags that are nested in parsed documents being used in an 'eval()' call, which could let a remote malicious user execute arbitrary PHP code. PHPXMLRPC : http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc.1.2.tgz?download Pear: http://pear.php.net/get/XML_RPC-1.4.0.tgz Drupal: http://drupal.org/files/projects/drupal-4.5.5.tar.gz eGroupWare: http://prdownloads.sourceforge.net/egroupware/eGroupWare-1.0.0.009.tar .gz?download MailWatch: http://prdownloads.sourceforge.net/mailwatch/mailwatch-1.0.2.tar.gz Nucleus: http://prdownloads.sourceforge.net/nucleuscms/nucleus-xmlrpc-patch.zip ?download RedHat: http://rhn.redhat.com/errata/RHSA-2005-748.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Mandriva: http://www.mandriva.com/security/advisories Gentoo: http://security.gentoo.org/glsa/glsa-200508-13.xml http://security.gentoo.org/glsa/glsa-200508-14.xml http://security.gentoo.org/glsa/glsa-200508-18.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Debian: http://security.debian.org/pool/updates/main/p/php4/ SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-20.xml http://security.gentoo.org/glsa/glsa-200508-21.xml Slackware: ftp://ftp.slackware.com/	PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution CAN-2005-2498	High	Security Focus, Bugtraq ID 14560, August 15, 2995 Security Focus, Bugtraq ID 14560, August 18, 2995 RedHat Security Advisory, RHSA-2005:748-05, August 19, 2005 Ubuntu Security Notice, USN-171-1, August 20, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:146, August 22, 2005 Gentoo Linux Security Advisory, GLSA 200508-13 & 14, & 200508-18, August 24 & 26, 2005 Fedora Update Notifications, FEDORA-2005-809 & 810, August 25, 2005 Debian Security Advisory, DSA 789-1, August 29, 2005 SUSE Security Announcement, SUSE-SA:2005:049, August 30, 2005 Gentoo Linux Security Advisory, GLSA GLSA 200508-20& 200508-21, August 30 & 31, 2005 Slackware Security Advisory, SSA:2005-242-02, August 31, 2005 Debian Security Advisory, DSA 798-1, September 2, 2005 SUSE Security Announcement, SUSE-SA:2005:051, September 5, 2005 **SGI Security Advisory, 20050901-01-U, September 7, 2005** **Slackware Security Advisories, SSA:2005-251-03 & 251-04, September 9,2005**

	pub/slackware/ Debian: http://security. debian.org/pool/ updates/main/p/ phpgroupware/ **SGI:** **ftp://oss.sgi.com/ projects/sgi_propack/ download/3/updates/** **Slackware:** **ftp://ftp.slackware.com/ pub/slackware/ slackware-current/ slackware/** **ftp://ftp.slackware.com/ pub/slackware/ slackware-10.1/ testing/packages/ php-5.0.5/php-5.0.5 -i486-1.tgz** There is no exploit code required.			
MyBB Group MyBulletinBoard 1.0 PR2	SQL injection vulnerabilities have been reported in 'misc.php' due to insufficient sanitization of the 'fid' parameter, in 'newreply.php' due to insufficient sanitization of the 'icon' parameter, and in 'ratethread.php' due to insufficient sanitization of the 'rating' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	MyBulletinBoard SQL Injection Vulnerabilities CAN-2005-2888	Medium	Secunia Advisory: SA16738, September 12, 2005
MySQL AB MySQL 5.0 .0-0-5.0.4, 4.1 .0-0-4.1.5, 4.0.24, 4.0.21, 4.0.20 , 4.0.18, 4.0 .0-4.0.15	A buffer overflow vulnerability has been reported due to insufficient bounds checking of data that is supplied as an argument in a user-defined function, which could let a remote malicious user execute arbitrary code. This issue is reportedly addressed in MySQL versions 4.0.25, 4.1.13, and 5.0.7-beta available at: http://dev.mysql.com/ downloads/ **Ubuntu:** **http://security.ubuntu.com/ ubuntu/pool/main/ m/mysql-dfsg/** **Mandriva:** **http://www.mandriva.com/ security/advisories** Currently we are not aware of any exploits for this vulnerability.	MySQL User-Defined Function Buffer Overflow	High	Security Focus 14509 , August 8, 2005 **Ubuntu Security Notice, USN-180-1, September 12, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:163, September 13, 2005**
OpenSSH OpenSSH 4.1, 4.0, p1	Several vulnerabilities have been reported: a vulnerability was reported due to an error when handling dynamic port forwarding when no listen address is specified, which could let a remote malicious user cause "GatewayPorts" to be incorrectly activated; and a vulnerability was reported due to an error when handling GSSAPI credential delegation, which could let a remote malicious user be delegated with GSSAPI credentials. Upgrades available at: ftp://ftp.openbsd.org/pub/ OpenBSD/OpenSSH/ openssh-4.2.tar.gz Fedora: http://download.fedora. redhat.com/pub/fedora/ linux/core/updates/3/ **Trustix:** **http://http.trustix.org/ pub/trustix/updates/** **Slackware:** **ftp://ftp.slackware.com/ pub/slackware/ slackware-current/**	OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials CAN-2005-2797 CAN-2005-2798	Medium	Secunia Advisory: SA16686, September 2, 2005 Fedora Update Notification, FEDORA-2005-858, September 7, 2005 **Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005** **Slackware Security Advisory, SSA:2005-251-03, September 9, 2005** **Fedora Update Notification, FEDORA-2005-860, September 12, 2005**

	Fedora: **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/** There is no exploit code required.			
OpenVPN OpenVPN 2.0 , 1.6 .0, 1.5 .0, 1.4.0-1.4.3, 1.3.2 , 1.2.1	Multiple remote Denial of Service vulnerabilities have been reported: a Denial of Service vulnerability was reported when flushing the OpenSSL error due to a failed client certificate authentication; a Denial of Service vulnerability was reported when flushing the OpenSSL error when a received packet fails to decrypt; a Denial of Service vulnerability was reported when configured in the 'dev tap' ethernet bridging mode; and a Denial of Service vulnerability was reported when two or more clients connect to the server at the same time using the same client certificate. Upgrades available at: http://openvpn.net/release/openvpn-2.0.1.tar.gz Mandriva: http://www.mandriva.com/security/advisories **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	OpenVPN Multiple Remote Denials of Service CAN-2005-2531 CAN-2005-2532 CAN-2005-2533 CAN-2005-2534	Low	Secunia Advisory: SA16463, August 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:145, August 22, 2005 **SUSE Security Summary Report, SUSE-SR:2005:020, September 12, 2005**
phpCommunity Calendar phpCommunity Calendar 4.0.3, 4.0.1, 4.0	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'webadmin/login.php' due to insufficient sanitization of the 'Username' parameter and in 'week.php' due to insufficient sanitization of the 'LocationID' parameter, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input passed to certain fields when adding an event, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported due to insufficient sanitization of the 'LocationID' and 'font' parameters in various scripts and in 'event.php' due to insufficient sanitization of the 'CeTi,' 'Contact,' 'Description,' and 'ShowAddress' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPCommunity Calendar Multiple Remote Vulnerabilities CAN-2005-2880 CAN-2005-2881 CAN-2005-2882	Medium	Secunia Advisory: SA16721, September 7, 2005
phpldapadmin phpldapadmin 0.9.6 - 0.9.7/alpha5	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported due to insufficient user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a Directory Traversal vulnerability was reported which could let a remote malicious user obtain sensitive information; and a file include vulnerability was reported, which could let a remote malicious user execute arbitrary PHP script code. No workaround or patch available at time of publishing. **An exploit script has been published.**	phpLDAPadmin Multiple Vulnerabilities CAN-2005-2792 CAN-2005-2793	Medium	Security Focus, Bugtraq ID: 14695, August 30, 2005 **Security Focus, Bugtraq ID: 14695, September 7, 2005**
PHPNuke PHPNuke 7.8	Multiple SQL injection vulnerabilities have been reported in the 'modules.php' due to insufficient sanitization of the 'name,' 'sid,' and 'pid' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPNuke Multiple SQL Injection	Medium	NewAngels Advisory #7, September 12, 2005
PunBB PunBB 1.2.1-1.2.6, 1.1-1.1.5, 1.0.1, 1.0, RC1 & RC2, beta1 - beta3, alpha	Multiple vulnerabilities have been reported: an SQL injection vulnerability was reported in the administration interface due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported due to insufficient sanitization of the BBcode 'url' tag , which could let a remote malicious user inject arbitrary script code; and an SQL injection vulnerability was reported due to insufficient sanitization of certain unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://www.punbb.org/	PunBB Multiple Vulnerabilities	Medium	Secunia Advisory: SA16775, September 12, 2005

	download/punbb-1.2.7.tar.gz There is no exploit code required.			
rdiff-backup rdiff-backup 1.0	A vulnerability has been reported when using the '-restrict,' '--restrict-read-only,' and '--restrict-update-only' options due to insufficient restriction of directory access, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://savannah.nongnu.org/download/rdiff-backup/rdiff-backup-1.0.1.tar.gz There is no exploit code required.	Rdiff-backup Directory Access Insufficient Restrictions	Medium	Security Focus, Bugtraq ID: 14804, September 12, 2005
SkyMinds.Net Mail-it Now! Upload2Server 1.5	A vulnerability has been reported in the attachment posting function because a remote malicious user can upload a file that contains arbitrary PHP code to the 'upload' directory. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Mail-it Now! Upload2Server Arbitrary File Upload	High	Security Tracker Alert ID: 1014884, September 12, 2005
SMC SMC7904WBRA	A remote Denial of Service vulnerability has been reported due to a failure to handle anomalous network traffic. No workaround or patch available at time of publishing. There is no exploit code required.	SMC SMC7904WBRA Wireless Router Remote Denial of Service	Low	Security Focus, Bugtraq ID: 14809, September 12, 2005
Spymac Spymac Web OS 4.0	A Cross-Site Scripting vulnerability has been reported in the 'index.php' script due to insufficient filtering of HTML code in the 'category' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Spymac Web OS Cross-Site Scripting	Medium	Security Tracker Alert ID: 1014883, September 12,2005
Stylemotion WEB//NEWS 1.4	SQL injection vulnerabilities have been reported in 'modules/startup.php' due to insufficient sanitization of the 'wn_userpw' parameter, in 'include_this/news.php' due to insufficient sanitization of the 'cat,' 'id,' and 'stof' parameters, and in 'print.php' due to insufficient sanitization of the 'id' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Stylemotion WEB//NEWS Multiple SQL Injection CAN-2005-2896 CAN-2005-2897	Medium	NewAngels Advisory #5, September 7, 2005
Subscribe Me Pro Subscribe Me Pro 2.44 .09P	A Directory Traversal vulnerability has been reported in 's.pl' due to insufficient sanitization, which could let a remote malicious user obtain sensitive information. Upgrade available at: http://siteinteractive.com/subpro/ There is no exploit code required; however, a Proof of Concept exploit has been published.	Subscribe Me Pro S.PL Remote Directory Traversal	Medium	Security Focus, Bugtraq ID: 14817, September 13, 2005
Sun Microsystems, Inc. Sun Java System Application Server Platform Edition 8.1 2005 Q1, UR1, Sun Java System Application Server Enterprise Edition 8.1 2005 Q1	A vulnerability has been reported because the contents of a JAR file can be exposed, which could let a remote malicious user obtain sensitive information. Upgrades available at: http://java.sun.com/j2ee/1.4/download.html There is no exploit code required.	Sun Java System Application Server JAR File Information Disclosure	Medium	Sun(sm) Alert Notification Sun Alert ID: 101905, September 13, 2005
Sun Microsystems, Inc. Sun Java Web Proxy Server 3.6, SP1-SP7	Three remote Denial of Service vulnerabilities have been reported when an unprivileged malicious user submits a specially crafted request. Updates available at: http://www.sun.com/download/products.xml?id=42fa5c49 Currently we are not aware of any exploits for these vulnerabilities.	Sun Java Web Proxy Server Remote Denials of Service	Low	Sun(sm) Alert Notification Sun Alert ID: 101913, September 8, 2005

Symantec Brightmail Anti-Spam 6.0.2	Several remote Denial of Service vulnerabilities have reported due to an error when scanning or cleaning certain messages and due to an error in the decomposer when processing messages that contain 'winmail.dat' objects that are embedded in a MIME file. Patch available at: ftp://ftp.symantec.com/public/english_us_canada/products/sba/sba_60x/updates/ Currently we are not aware of any exploits for these vulnerabilities.	Symantec Brightmail Remote Denials of Service	Low	Secunia Advisory: SA16733, September 7, 2005
tDiary tDiary 2.1.1, 2.0.1	A vulnerability has been reported due to a failure to perform validity checks on user's requests, which could let a remote malicious user edit/delete entries or configurations. Upgrades available at: http://prdownloads.sourceforge.net/tdiary/tdiary-full-2.0.2.tar.gz?download **Debian:** **http://security.debian.org/pool/updates/main/t/tdiary/** There is no exploit code required.	TDiary Cross-Site Request Forgery CAN-2005-2411	Medium	Security Focus, 14500, August 8, 2005 **Debian Security Advisory, DSA 808-1, September 12, 2005**
Unclassified NewsBoard Unclassified NewsBoard 1.5.3	A vulnerability has been reported in the Description field due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. **Patch available at:** **http://newsboard.unclassified.de/release/update/patch-1.5.3-a.diff** There is no exploit code required; however, a Proof of Concept exploit has been published.	Unclassified NewsBoard Description Field HTML Injection CAN-2005-2883	Medium	Security Focus, Bugtraq ID: 14748, September 6, 2005 **Security Focus, Bugtraq ID: 14748, September 14, 2005**
Zebedee Zebedee 2.4.1	A remote Denial of Service vulnerability has been reported due to a failure to handle exceptional network requests. Upgrades available at: http://prdownloads.sourceforge.net/zebedee/zebedee-2.4.1A.tar.gz?downl oad There is no exploit code required; however, an exploit script has been published.	Zebedee Remote Denial of Service CAN-2005-2904	Low	Secunia Advisory: SA16788, September 12, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **Users beware: pirates nearby:** In recent months law enforcement authorities nationwide have noticed a problem with Wi-Fi networks, Wi-Fi pirates. Without proper security, it is possible for malicious users to tap your wireless Internet signal. If you are vulnerable, Wi-Fi pirates can use your wireless signal to surf the Net on your dime. In the worst cases, strangers outside your home or just down the street may monitor where you go on the Net, read your e-mails or access your personal information. Source: http://www.crime-research.org/news/13.09.2005/1489/

Wireless Vulnerabilities

- SMC SMC7904WBRA Wireless Router Remote Denial of Service: A remote Denial of Service vulnerability has been reported due to a failure to handle anomalous network traffic.
- Linksys WRT54G Wireless Router Multiple Remote Vulnerabilities: Multiple vulnerabilities have been reported which could let a remote malicious user bypass security restrictions, cause a Denial of Service or potentially compromise a vulnerable system.
- BlueZ Arbitrary Command Execution: A vulnerability has been reported due to insufficient sanitization of input passed as a remote device name, which could let a remote malicious user execute arbitrary code. Updated information regarding Conectiva patch.
- btscanner-2.0.tar.bz2: A tool that extracts as much information as possible from a Bluetooth device without the requirement to pair.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script	Script name	Workaround or	Script Description

(Reverse Chronological Order)		Patch Available	
September 14,2005	btscanner-2.0.tar.bz2	N/A	A tool that extracts as much information as possible from a Bluetooth device without the requirement to pair. A detailed information screen extracts HCI and SDP information, and maintains an open connection to monitor the RSSI and link quality.
September 13, 2005	azdgexpl.php	No	Exploit for the Azerbaijan Development Group AZDGDatingLite Directory Traversal vulnerability.
September 13, 2005	cjXSS.txt	No	Exploitation details for the CjTagBoard 3.0, CjLinkOut 1.0, and CjWeb2Mail 3.0 Cross-Site Scripting vulnerability.
September 13, 2005	firefoxIDN.txt	Yes	Working exploit for the Firefox IDN Buffer Overrun vulnerability.
September 13, 2005	mailitnow.html	No	Exploitation details for the Mail-it Now! Upload2Server Arbitrary File Upload vulnerability.
September 13, 2005	Mail-it-Now-expl.php	No	Script that exploits the Mail-it Now! Upload2Server Arbitrary File Upload vulnerability.
September 13, 2005	nmap-3.93.tgz	N/A	A utility for port scanning large networks.
September 13, 2005	snortrigger.c	No	Script that exploits the Snort PrintTcpOptions Remote Denial of Service vulnerability.
September 12, 2005	COOL_poc.pl	No	Proof of Concept exploit for the COOL! Remote Control Remote Denial of Service vulnerability.
September 12, 2005	imap4d_search_expl.c	Yes	Script that exploits the GNU Mailutils Format String vulnerability.
September 12, 2005	phptagcool-sql.pl	No	Perl script that exploits the Crashcool.com PhpTagCool SQL Injection vulnerability.
September 9, 2005	KillProc_PoC.exe	No	Proof of Concept exploit for the KillProcess Buffer Overflow vulnerability.
September 9, 2005	mkZebedeeDoS.c	Yes	Script that exploits the Zebedee Remote Denial of Service vulnerability.
September 8, 2005	Class-1_poc class1.html	No	Proof of Concept exploit for the Class-1 Forum SQL Injection Vulnerability.
September 8, 2005	mimedefang-2.53.tar.gz	N/A	A flexible MIME email scanner designed to protect Windows clients from viruses that includes the ability to do many other kinds of mail processing, such as replacing parts of messages with URLs. It can alter or delete various parts of a MIME message according to a very flexible configuration file.
September 8, 2005	MyBBPR2.txt	No	Exploit details for the MyBB SQL injection vulnerability.
September 8, 2005	pblang465.php.txt	Yes	Exploit for the PBLang Multiple Vulnerabilities.
September 7, 2005	phpLDAPadmin-exec.pl	No	Perl script that exploits the phpLDAPadmin Multiple Vulnerabilities.

[back to top]

Trends

- **One In Six Spyware Apps Tries To Steal Identities:** According to a security firm, a significant portion of spyware is designed to steal identities. This indicates a trend toward more malicious use of such software by criminals. Fifteen percent of the 2,000 known spyware threats analyzed by Aladdin Knowledge Systems over a two-month span send private information gathered from the infected PC by logging keystrokes, capturing usernames and passwords, and hijacking e-mail address and contact lists. Source: http://www.techweb.com/wire/security/170703179
- **Bot herder websites in internet take-down:** According to anti-virus firm, F-Secure high profile bot sites such as ryan1918.com and 0x90-team.com have disappeared. Source: http://www.theregister.co.uk/2005/09/13/bot_herder_takedown/.
- **Businesses And Networks Are Unprepared For Disasters: AT&T Survey:** According to a new report done by AT&T and the International Association of Emergency Managers (IAEM) suggests that many enterprise networks are not prepared for disasters and a large proportion of companies have made continuity planning a low priority. The study, "Disaster Planning in the Private Sector: A Look at the State of Business Continuity in the U.S.," found that almost one third of U.S. businesses do not have continuity plans, and that nearly 40% of the 1200 companies surveyed reported that continuity planning was not a priority. More than 40% of the companies surveyed do not have off-site back-up or redundant servers and almost a third have failed to implement basic network security measures. Source: http://nwc.networkingpipeline.com/news/170702684.
- **Research: E-Mail Remains A Point Of Vulnerability:** Messaging Security Market Trends 2005-2008 study finds that businesses face a large number of messaging problems. Of the 115 companies surveyed, two-thirds struggle to provide adequate storage for E-messages and archiving. Nearly all surveyed companies have had their networks successfully penetrated by a virus, worm, or other form of malware through E-mail. Source: http://www.messagingpipeline.com/170702394.
- **Katrina victims at risk for ID theft, experts say:** According to experts, important and sensitive document left behind in the waterlogged debris of Hurricane Katrina could put the storm's victims at a risk for identify theft. U.S. officials and consumer advocates said they had not yet heard of any cases of identity theft related to the disaster because the crime usually takes months to unfold. Source: http://today.reuters.com/news/newsArticle.aspx?type=technologyNews&storyID=2005-09-08T210539Z_01_BAU875711_RTRIDST_0_TECH-IDTH .
- **Nigerian Scams Spin Katrina Disaster:** According to Kaspersky Labs, Nigerian-style scams are beginning to appear that use the Katrina disaster. Source: http://www.techweb.com/wire/security/170701190 .
- **US losing battle against identity theft:** According to the Identity Theft Resource Center (ITRC) there have been at least 104 serious "data incidents" in the US since 1 January. The incidents potentially affect more than 56.2 million individuals. Source: http://www.vnunet.com/vnunet/news/2141968/losing-battle-against-theft.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
3	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.
4	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
5	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
6	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality that can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
7	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
8	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
9	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
10	Mytob-BE	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.

Table updated September 12, 2005

[back to top]

Last updated September 15, 2005